IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of:

receiving at a transparent proxy a request from a client requesting a resource of an origin server, wherein the transparent proxy is unknown to the client;

redirecting the client request from the transparent proxy to a policy module;

obtaining at the transparent proxy policy enforcement data, wherein the policy enforcement data is received from the policy module and wherein the policy module and the transparent proxy reside within a same environment;

generating at the transparent proxy a policy state token in response to the policy enforcement data; and transmitting the policy state token from the transparent proxy to the client, wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy.

2. (Previously Presented) The method of claim 1, further comprising the step of receiving at the transparent proxy a renewed request for the origin server resource, the renewed request containing the policy state token.

3. (Previously Presented) The method of claim 2, wherein the renewed request contains the policy state token in a cookie in a header sent from the client to the transparent proxy.

4. (Original) The method of claim 2, further comprising the step of forwarding to the origin server a portion of the renewed request, the forwarded portion omitting the policy state token.

5. (Previously Presented) The method of claim 4, further comprising the step of receiving at the transparent proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server.

6. (Previously Presented) The method of claim 4, further comprising the steps at the transparent proxy of forwarding to the client at least a portion of a communication from the origin server, and forwarding to the origin server at least a portion of a communication from the client.

7. (Original) The method of claim 1, wherein HTTP is a protocol used during at least one of the receiving and transmitting steps.

8. (Original) The method of claim 1, wherein HTTPS is a protocol used during at least one of the receiving and transmitting steps.

9. (Previously Presented) The method of claim 1, wherein the method further comprises utilizing Novell Directory Services software to provide authentication information about the client, and the transparent policy enforcement data obtained by the transparent proxy depends on the authentication information thus provided.

10. (Previously Presented) The method of claim 1, wherein the method further comprises utilizing Lightweight Directory Access Protocol software to provide authentication information about the client, and the policy enforcement data obtained by the transparent proxy depends on the authentication information thus provided.

11. (Previously Presented) The method of claim 1, wherein the method further comprises utilizing Secure Sockets Layer software to provide authentication information about the client, and the policy enforcement data obtained by the transparent proxy depends on the authentication information thus provided.

12. (Original) The method of claim 1, wherein the obtaining step extracts policy enforcement data from a redirection address field.

13. (Previously Presented) The method of claim 1, wherein the transmitting step transmits the policy state token in a cookie in a header sent from the transparent proxy to the client.

14. (Currently Amended) A transparent proxy server comprising:

a memory configured at least in part by a transparent proxy process;

a processor for running the transparent proxy process;

at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand; and

a policy module identifier which identifies a policy module that grants or denies authorization of proxy services to the client computer by acquiring policy enforcement data and attempting to authenticate the client computer to the transparent proxy process in response to the policy enforcement data, and wherein the client computer directs a request for a resource to an origin server and the request is intercepted by the transparent proxy process, which is unknown to the client computer, and used to determine the policy module identifier which identifies the policy module, and wherein the policy module authenticates the client computer to the transparent proxy process for subsequent interactions between the client computer and the transparent proxy process, and wherein the policy module processes within a same environment as the transparent process.

15. (Original) The transparent proxy server of claim 14, in combination with the policy module.

16. (Original) The transparent proxy server of claim 15, wherein the policy module and the transparent proxy process are running on the same computer.

17. (Original) The transparent proxy server of claim 14, in combination with the client computer and at least one other client computer, each client computer linked for networked communication with the transparent proxy process.

18. (Previously Presented) The transparent proxy server of claim 14, wherein the transparent proxy server provides authorized proxy service transparently to both the client computer and the origin server by steps which comprise receiving the request from the client for the resource of the origin server, sending the client computer an authorization by the policy module for the client computer to use a transparent proxy service, accepting the authorization from the client computer with a renewed client request for the origin server resource, forwarding the renewed client request to the origin server without forwarding the authorization but with an indication to the origin server that the transparent proxy server is the source of the forwarded request, and then transparently forwarding the requested resource from the origin server to the client computer.

19. (Previously Presented) The transparent proxy server of claim 18, wherein the transparent proxy server send the client computer the authorization by sending the client computer a proxy cookie for use in subsequent communications from the client computer.

20. (Original) The transparent proxy server of claim 14, in combination with at least one additional transparent proxy server which also has a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, a link, and a policy module identifier.

21. (Previously Presented) The combined transparent proxy servers of claim 20, wherein one transparent proxy server forwards other client requests to the other transparent proxy server.

22. (Original) The combined transparent proxy servers of claim 20, wherein one transparent proxy server takes over the handling of client requests in place of the other transparent proxy server.

23. (Currently Amended) A pair of state information brokering signals embodied in a distributed computer system, the system containing a client, a transparent proxy server having a transparent proxy server address, and a policy module having a policy module address, the pair of signals comprising:

a first signal including a redirection command which specifies the policy module address as a redirection target; and

a second signal including a redirection command which specifies the transparent proxy server address as a redirection target and also including policy enforcement data which grants or denies authorization for the client to use a service of the transparent proxy server, and wherein the transparent proxy server controls access to the service based on client authentication to the proxy service achieved through the policy enforcement data, the first and second signal originating within a same environment that is external to the client, and wherein the transparent proxy server is unknown to the client.

24. (Original) The signal pair of claim 23, wherein the first signal includes an identity broker address as the policy module address.

25. (Original) The signal pair of claim 23, wherein the first signal includes a login server address as the policy module address.

26. (Original) The signal pair of claim 23, wherein the second signal includes the policy enforcement data embedded in an address field with the transparent proxy server address.

27. (Currently Amended) A computer storage medium having a configuration that represents data and instructions which will cause performance of method steps for transparent proxy services, the method comprising the steps of:

receiving at a transparent proxy a request from a client requesting a resource of an origin server, wherein the transparent proxy is unknown to the client;

redirecting the client request from the transparent proxy to a policy module; and

obtaining at the transparent proxy policy enforcement data provided by the policy module, the policy enforcement data granting or denying authorization for the client to access the resource through the transparent proxy, wherein the policy enforcement data is directed to authenticating the client to the transparent proxy and the transparent proxy vends access to the resource, and wherein the policy module and the transparent process execute within a same environment that is external to the client.

28. (Original) The configured storage medium of claim 27, wherein the policy enforcement data grants authorization for the client to access the resource through the transparent proxy, and the method further comprises the steps of generating at the transparent proxy a proxy cookie containing at least a portion of the policy enforcement data, and transmitting the proxy cookie from the transparent proxy to the client.

29. (Original) The configured storage medium of claim 28, wherein the method further comprises the steps of accepting the proxy cookie at the transparent proxy with a renewed client request for the origin server resource, and forwarding the renewed client request to the origin server without the proxy cookie.

30. (Original) The configured storage medium of claim 29, wherein the method further comprises the step of transparently forwarding the requested resource from the origin server to the client.

31. (Original) The configured storage medium of claim 27, wherein the transparent proxy is a first transparent proxy, the policy enforcement data includes first policy enforcement data which grants authorization for the client to access the resource through the first transparent proxy, and the method further comprises the steps of:

generating at the first transparent proxy a proxy cookie in response to the first policy enforcement data;

transmitting the proxy cookie from the first transparent proxy to the client;

receiving the first proxy cookie from the client at a second transparent proxy with a renewed client request for the origin server resource, after the first transparent proxy becomes unavailable to the client;

redirecting the renewed client request from the second transparent proxy to a policy module; and

accepting, at the second transparent proxy, the second policy enforcement data provided by the policy module, the second policy enforcement data including authorization from the policy module for the client to access the resource through the second transparent proxy.